UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,127	01/14/2000	Alan Dowd	105.176US1	7964

21186	7590	05/24/2006

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER
CRAIG, DWIN M

ART UNIT	PAPER NUMBER
2123	

DATE MAILED: 05/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

		Application No.	Applicant(s)
Office Action Summary		09/483,127	DOWD ET AL.
		Examiner	Art Unit
		Dwin M. Craig	2123

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>27 February 2006</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-42</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-25, 27-31, 33-36 and 38-42</u> is/are rejected.

7)☒ Claim(s) <u>26, 32 and 37</u> is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>1/14/2000</u> is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1.   In view of the Appeal Brief filed on 2-27-2006, PROSECUTION IS HEREBY

REOPENED. New grounds of rejection to the Appeal Brief set forth below.

Response to Arguments

2.   Applicant's arguments with respect to claims 1-42 have been considered but are moot in

view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

The text of those sections of Title 35, U.S. Code not included in this action can be found

in a prior Office action.

This application currently names joint inventors. In considering patentability of the

claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various

claims was commonly owned at the time any inventions covered therein were made absent any

evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out

the inventor and invention dates of each claim that was not commonly owned at the time a later

invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c)

and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

3.   Claims 1-8 and 18-20 are rejected under 35 USC § 103(a) as being unpatentable over US

Patent 6,014,697 *Lewis* in view of US Patent 6,298,445 *Shostack*.

3.1   As regards independent claims 1 and 18 and using independent claim 1 as an example,

Lewis discloses *a network configuration module having network configuration data* (Figure 1

reference 18, Col. 2 lines 4-6, 21-36, Figure 2 reference 42), and *a simulator* (Figure 1 reference

36, Col. 3 lines 17-24 and Col. 2 lines 51-56), *coupled to the network configuration module*

(Figure 1 references 34 and 36), *to simulate and analyze networks based on the network*

configuration data (Col. 1 lines 39-52).

However *Lewis* does not expressly disclose the database having *network vulnerabilities,*

defense conditions that might close the vulnerability, and resource and state conditions needed

to exercise the vulnerability.

Shostack discloses a database that contains, *network vulnerabilities* (Figure 5 reference

92), *defense conditions that might close the vulnerability* (Col. 2 lines 48-54, "a database of

known security <u>vulnerabilities</u>"), *and resource and state conditions needed to exercise the*

vulnerability (Col. 6 lines 53-65, the Examiner notes that, "electronically disengage(ing) the

intruder" will exercise a vulnerability).

It would have been obvious, to one of ordinary skill in the art, at the time the invention

was made to have used the *network vulnerabilities database* of *Shostack* with the *network*

simulation database of *Lewis* because of the advantages provided by the database of *Shostack* to

prevent damage to a computer network and systems (see *Shostack* Col. 2 lines 18-28).

3.2   As regards dependent claim 2, *Lewis* does not expressly disclose network vulnerability,

attack and exploitation data however, *Shostack* discloses network vulnerability, attack and

exploitation data (Col. 2 lines 48-67 and Col. 3 lines 1-37).

3.3   As regards dependent claim 3, *Lewis* discloses a *database*, which contains tables, and the

database of *Lewis* is being executed on a computer (Figure 1).

3.4   As regards dependent claim 4, *Lewis* discloses *output of data from a network discovery*

tool (Figure 1 references 14, 18, 20 and 22).

3.5   As regards dependent claim 5, *Lewis* discloses a *user interface* (Figure 1 references 22

and 40).

3.6   As regards dependent claim 6, *Lewis* does not expressly disclose *a means for receiving*

the network vulnerability, attack and exploitation data.

    Shostack discloses *a means for receiving the network vulnerability, attack and*

exploitation data (Figure 7).

3.7   As regards dependent claim 7, *Lewis* does not expressly disclose an *attacker and a*

defender interface.

    Shostack discloses the functional equivalent of an *attacker and defender interface* (Figure

1 reference(s) 8 and 16).

3.8   As regards dependent claim 8 *Lewis* discloses a *"portable"* security modeling system,

more specifically in Col. 4 lines 29-39 disclose the use of the *Sniffer by Network General*

Corporation, it is known through the personal knowledge of the Examiner that the *Sniffer*

product is provided on stand alone *portable* computer systems as well as CDROM encoded

computer readable media that can be utilized on *portable* computer systems.

3.9   As regards dependent claim 19 *Lewis* discloses a *network discovery tool* (Figure 1

reference 14).

3.10   As regards dependent claim 20 *Lewis* discloses *receiving a file* (Figure 1 references 24,

26, 28, 30, 32 and 34 and Col. 3 lines 25-33).

4.   Claims 10-25, 27-31, 33-36 and 40-42 are rejected under 35 USC § 103(a) as being

unpatentable over US Patent 6,014,697 *Lewis* in view of US Patent 6,408,391 *Huff.*

4.1   As regards independent claims 10, 18, 28, 34 and 40 and using independent claim 10 as

an example, *Lewis* discloses *a network configuration module having network configuration data*

(Figure 1 reference 18, Col. 2 lines 4-6, 21-36, Figure 2 reference 42), and *a simulator* (Figure 1

reference 36, Col. 3 lines 17-24 and Col. 2 lines 51-56), *coupled to the network configuration*

module (Figure 1 references 34 and 36), *to simulate and analyze networks based on the network*

configuration data (Col. 1 lines 39-52).

         However, *Lewis* dos not expressly disclose *a mission objective module, with critical*

resource information and specific attack scenarios.

         Huff discloses *a mission objective module, with critical resource information and specific*

attack scenarios (Abstract, Figure 3 references 320, 322 and 324, Col. 3 lines 49-58, Col. 8 lines

34-56, Col. 9 lines 6-17, Col. 10 lines 3-67, Col. 11 lines 1-6, Col. 11 lines 22-67 and Col. 12

lines 1-24).

         It would have been obvious, to one of ordinary skill in the art, at the time the invention

was made to have used the teachings of *Huff* with the *network configuration and simulator*

database methods of Lewis to protect a network from cyber attacks because, *prior art systems*

can be circumvented before a human system administrator takes action (*Huff,* Col. 11 lines 2-6)

thus, having an automated network protection system provides for better network security and

protection of critical data.

4.2   As regards dependent claim 11 *Lewis* does not expressly disclose *network vulnerability,*

attack and exploitation data.

>   *Huff* discloses *network vulnerability, attack and exploitation data* (Col. 7 lines 52-65).

4.3   As regards dependent claim 12 *Lewis* does not expressly disclose *network vulnerability,*

attack and exploitation data is stored in database tables processed by a computer.

Huff discloses a database with network vulnerability data, attack data and exploitation

data, stored and processed by a computer (Figure 3 reference 286).

4.4   As regards dependent claim 13 *Lewis* discloses a *GUI* (Col. 2 lines 51-56).

4.5   As regards dependent claim 14 *Lewis* discloses *goals, expectations and constraints for*

simulating a network (Col. 1 lines 39-53).

4.6   As regards dependent claim 15 *Lewis* discloses *means for receiving network data* (Figure

1 reference 16).

4.7   As regards dependent claim 16 a *Lewis* discloses a *"portable"* security modeling system,

more specifically in Col. 4 lines 29-39 disclose the use of the *Sniffer by Network General*

Corporation, it is known through the personal knowledge of the Examiner that the *Sniffer*

product is provided on stand alone *portable* computer systems as well as CDROM encoded

computer readable media that can be utilized on *portable* computer systems.

4.8   As regards dependent claim 17 *Lewis* does not expressly disclose *attackers and*

defenders.

Huff discloses *attackers and defenders* (Col. 2 lines 58-65, *et seq.*) *Huff* also discloses a

GUI for the defender (Col. 7 lines 45-47).

4.9   As regards dependent claim 19 *Lewis* discloses a *network discovery tool* (Figure 1

reference 14).

4.10   As regards dependent claim 20 *Lewis* discloses *receiving a file* (Figure 1 references 24,

26, 28, 30, 32 and 34 and Col. 3 lines 25-33).

4.11   As regards dependent claim 21, *Lewis* does not expressly disclose *receiving mission*

objectives, storing and simulating a network based on those objectives.

Huff discloses *receiving mission objectives, storing and simulating a network based on*

those objectives (Col. 9 lines 6-17, Col. 9 lines 33-53, Col. 10 lines 33-44, "increase the auditing

level being performed by the intrusion detection mission", *et seq.*).

4.12   As regards dependent claim 22, *Lewis* does not expressly disclose modifying a GUI.

Huff discloses modifying a GUI based on activity on the network (Figure 4, Col. 7 lines

45-47).

4.13   As regards dependent claims 23-25 *Lewis* does not expressly disclose dynamic

interaction with an attacker.

Huff discloses dynamically interacting with an attacker, in real time and interacting with

the security modeling system (Col. 2 lines 64-66, Col. 3 lines 23-29, Col. 7 lines 52-65 *et seq.*).

4.14   As regards dependent claim 27 *Lewis* discloses updating a database (Figure 1 reference

34 and Figure 2 reference 48, Col. 3 lines 29-33).

4.15   As regards dependent claim 29 *Lewis* does not expressly disclose receiving information

from a defender.

Huff discloses receiving information from a defender (Col. 11 lines 23-45).

4.16   As regards dependent claim 30 *Lewis* discloses *goals, expectations and constraints for simulating a network* (Col. 1 lines 39-53).

4.17   As regards dependent claim 31 *Lewis* does not expressly disclose modifying a GUI.

Huff discloses modifying a GUI based on activity on the network (Figure 4, Col. 7 lines 45-47).

4.18   As regards dependent claim 33 *Lewis* does not expressly disclose receiving commands.

Huff discloses *receiving commands to change the attacker/defender nodes, service functionality and exploit vulnerabilities* (Figure 3-5 and in figure 5 reference 272 and 272' "response engines" which send commands to the "agents" Col. 13 lines 30-43).

4.19   As regards dependent claims 35 and 36, *Lewis* does not expressly disclose *mission objective tables, mission files tables and mission service tables.*

Huff discloses a database (Figure 3 reference 286, Figure 5 references 300 and 300' and Col. 7 lines 18-65), the Examiner notes that all databases have tables or data stored in tabular format. *Huff* further discloses the functional equivalent of *mission objective tables, mission files tables and mission service tables* (Col. 9 lines 54-67, Col. 10 and Col. 11 liens 1-6, *et seq.*).

4.20   As regards dependent claims 41 and 42, *Lewis* does not expressly disclose *mission objectives.*

Huff discloses *mission objectives* (Col. 11 lines 22-45).

5.   Claims 9, 38 and 39 are rejected under 35 USC § 103(a) as being unpatentable over US Patent 6,014,697 *Lewis* in view of US Patent 6,408,391 *Huff* and in further view of Official Notice.

5.1   As regards independent claim 9, *Lewis* discloses *a network configuration module having*

network configuration data (Figure 1 reference 18, Col. 2 lines 4-6, 21-36, Figure 2 reference

42), and *a simulator* (Figure 1 reference 36, Col. 3 lines 17-24 and Col. 2 lines 51-56), *coupled*

to the network configuration module (Figure 1 references 34 and 36), *to simulate and analyze*

networks based on the network configuration data (Col. 1 lines 39-52).

However *Lewis* does not expressly disclose the *database having network vulnerabilities*.

Huff discloses *a database having network vulnerabilities* (Col. 7 lines 52-65). *Huff* also

discloses an interactive GUI (Figure 4, Col. 7 lines 45-60).

It would have been obvious, to one of ordinary skill in the art, at the time the invention

was made to have used the teachings of *Huff* with the *network configuration and simulator*

database methods of Lewis to protect a network from cyber attacks because, *prior art systems*

can be circumvented before a human system administrator takes action (*Huff*, Col. 11 lines 2-6)

thus, having an automated network protection system provides for better network security and

protection of critical data.

Official Notice...

As regards the limitation of independent claim 9 that the simulator is used as a game.

At the time the invention was made *Real Time Simulation (RTS) Games* where widely

available, more specifically games like *StarCraft®* and *Warcraft II®* by *Blizzard®*

Entertainment Inc. were available and disclosed interactive simulation(s) where an attacker and a

defender could attack each other using a GUI over a network. More specifically, *Blizzard®*

Entertainment Inc. actually provided specific network servers to facilitate these networked

games known as *Battle.net®* servers, therefore, it would have been obvious, to one of ordinary

skill in the art, at the time the invention was made to have taken the claimed invention and use the *network simulator* as a *RTS* game.

5.2   As regards dependent claim 38, *Lewis* does not expressly disclose an *attacker* interface.

However, *Huff* discloses an *attacker interface* (Figure 1 reference 130) and a *Defender interface* (Figure 4, Col. 7 lines 45-60).

5.3   As regards dependent claim 39 *Lewis* does not expressly disclose *mission objectives.*

Huff discloses *receiving mission objectives, storing and simulating a network based on those objectives* (Col. 9 lines 6-17, Col. 9 lines 33-53, Col. 10 lines 33-44, "increase the auditing level being performed by the intrusion detection mission", *et seq.*).

Allowable Subject Matter

6.   Claims 26, 32 and 37 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

6.1   As regards dependent claims 26 and 32, the following limitations are neither anticipated nor made obvious by the prior art, *"wherein determining the vulnerabilities includes computing results which include a security score"*.

6.2   As regards dependent claim 37 the following combination of limitations are neither anticipated nor made obvious by the prior art *"defense tables, filter tables, node tables, routing tables and password tables"*.

Conclusion

7.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Dwin M. Craig whose telephone number is (571) 272-3710. The

examiner can normally be reached on 10:00 - 6:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Paul L. Rodriguez can be reached on (571) 272-3753. The fax phone number for the

organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DMC

Primary Examiner
Art Unit 2125 2123